

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-237186

(P2003-237186A)

(43) 公開日 平成15年8月27日 (2003.8.27)

(51) Int.Cl. ⁷	識別記号	F I	テームト (参考)
B 4 1 J 29/38		B 4 1 J 29/38	Z 2 C 0 6 1
5/30		5/30	Z 2 C 1 8 7
29/00		G 0 6 F 3/12	K 5 B 0 2 1
G 0 6 F 3/12		G 0 6 T 1/00	5 0 0 B 5 B 0 5 7
G 0 6 T 1/00	5 0 0	H 0 4 N 1/00	B 5 C 0 6 2
審査請求 未請求 請求項の数20 O L (全 12 頁) 最終頁に続く			

(21) 出願番号 特願2002-41695 (P2002-41695)

(22) 出願日 平成14年2月19日 (2002.2.19)

(71) 出願人 000000295

沖電気工業株式会社

東京都港区虎ノ門1丁目7番12号

(72) 発明者 永重 務

東京都港区虎ノ門1丁目7番12号 沖電気
工業株式会社内

(72) 発明者 村瀬 嘉史

東京都港区虎ノ門1丁目7番12号 沖電気
工業株式会社内

(74) 代理人 100095957

弁理士 亀谷 美明 (外2名)

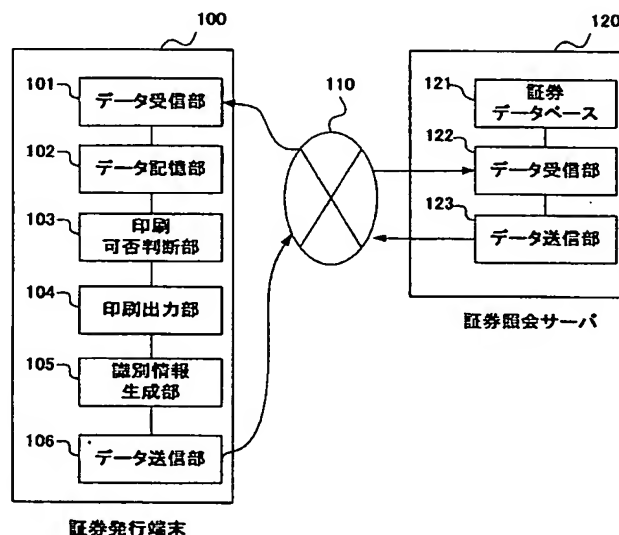
最終頁に続く

(54) 【発明の名称】 印刷物発行端末、サーバ、及び印刷物発行方法

(57) 【要約】

【課題】 手形、小切手、証券等の印刷物を出力するにあたり、画像データの漏洩、改竄、印刷された証券の複製、改竄等の不正行為を防止する印刷物発行端末、サーバ、及び印刷物発行方法を提供する。

【解決手段】 サーバ120へ照会したデータベース121にある画像データを、ネットワーク110を介して証券発行端末100のデータ受信部101で受信し、これをデータ記憶部102が記憶し、印刷可否判断部103は印刷済み識別情報が存在すれば印刷不可と、存在しなければ印刷可と判断し、印刷出力部104より証券を印刷出力する。また、印刷出力後に識別情報生成部105は証券の印刷済み識別情報を生成し、これをネットワーク110を介して証券照会サーバ120へ送信する。印刷後にデータ記憶部102の証券画像データは削除される。



【特許請求の範囲】

【請求項 1】 ネットワークを介して画像データをサーバから受信するデータ受信部と、前記画像データから印刷済み識別情報を抽出し、前記印刷済み識別情報が存在すれば印刷不可と判断し、前記印刷済み識別情報が存在しなければ印刷可と判断する印刷可否判断部と、前記印刷可否判断部の判断に従い、前記画像データに基づいて印刷物を出力する印刷出力部と、前記印刷物を出力した後に、前記画像データの印刷済み識別情報を生成する識別情報生成部と、前記生成した印刷済み識別情報を、ネットワークを介して前記サーバへ送信するデータ送信部とを有することを特徴とする印刷物発行端末。

【請求項 2】 更に、前記サーバから受信した画像データを記憶するデータ記憶部と、前記データ記憶部に記憶された画像データを削除するデータ削除部とを有し、前記印刷出力部は、前記データ記憶部に記憶された画像データに基づいて印刷物を出力するとともに、前記データ削除部は、前記印刷出力部が印刷物を出力した後に、前記データ記憶部に記憶された画像データを削除することを特徴とする請求項 1 に記載の印刷物発行端末。

【請求項 3】 前記識別情報生成部が生成する印刷済み識別情報は、前記画像データから生成された電子署名データを少なくとも含むことを特徴とする請求項 1 または 2 のうちのいずれか 1 項に記載の印刷物発行端末。

【請求項 4】 前記電子署名データは、ハッシュ関数を利用して前記画像データから生成されることを特徴とする請求項 3 に記載の印刷物発行端末。

【請求項 5】 前記データ送信部が送信する印刷済み識別情報は、前記画像データの通し番号、及び／または、印刷物発行端末番号を更に含むことを特徴とする請求項 3 または 4 のうちのいずれか 1 項に記載の印刷物発行端末。

【請求項 6】 特定の情報を電子透かしとして前記画像データに埋め込む電子透かし埋め込み部を更に有し、前記印刷出力部は、電子透かしを埋め込んだ印刷物を出力することを特徴とする請求項 1、2、3、4、または 5 のうちのいずれか 1 項に記載の印刷物発行端末。

【請求項 7】 前記サーバより受信した、公開鍵暗号方式によって暗号化された画像データを復号する復号部を更に有し、前記暗号化された画像データを前記復号部が復号する際に、ICカード、パスワード、または、バイオメトリクスによって利用者の認証が行われることを特徴とする請求項 1、2、3、4、5、または 6 のうちのいずれか 1 項に記載の印刷物発行端末。

【請求項 8】 前記電子透かしを用いて改竄検出を行う改竄検出部を更に有し、前記改竄検出部が前記画像データの改竄を検出したときに、前記データ送信部は改竄検出情報を前記サーバへ送信することを特徴とする請求項 1、2、3、4、5、6 または 7 のうちのいずれか 1 項に記載の印刷物発行端末。

【請求項 9】 画像データを保存するデータベースと、印刷物発行端末からの照会情報、及び、前記印刷物発行端末が生成した印刷済み識別情報を、前記印刷物発行端末よりネットワークを介して受信するデータ受信部と、ネットワークを介して、前記印刷物発行端末からの照会情報に応じて前記データベースに保存される画像データと、前記印刷物発行端末により生成された印刷済み識別情報が既に存在している場合に、当該印刷済み識別情報とを、前記印刷物発行端末へ送信するデータ送信部とを有することを特徴とするサーバ。

【請求項 10】 前記データ送信部が送信する印刷済み識別情報は、少なくとも前記画像データから生成された電子署名データを含むことを特徴とする請求項 9 に記載のサーバ。

【請求項 11】 前記電子署名データは、ハッシュ関数を利用して前記画像データから生成されたことを特徴とする請求項 10 に記載のサーバ。

【請求項 12】 前記データ送信部が送信する印刷済み識別情報は、前記画像データの通し番号、及び／または、印刷物発行端末番号を更に含むことを特徴とする請求項 10 または 11 のうちのいずれか 1 項に記載のサーバ。

【請求項 13】 特定の情報を電子透かしとして前記画像データに埋め込む電子透かし埋め込み部を更に有し、前記電子透かしを埋め込んだ画像データを前記データ送信部よりネットワークを介して印刷物発行端末に送信する機能を有することを特徴とする請求項 9、10、11、または 12 のうちのいずれか 1 項に記載のサーバ。

【請求項 14】 前記画像データを公開鍵暗号方式によって暗号化する暗号化部を更に有することを特徴とする請求項 9、10、11、12、または 13 のうちのいずれか 1 項に記載のサーバ。

【請求項 15】 前記暗号化部は、認証局が発行する公開鍵証明書が証明する公開鍵を用いることを特徴とする請求項 14 に記載のサーバ。

【請求項 16】 ネットワークを介して画像データをサーバから印刷物発行端末へ送信する段階と、前記画像データから印刷済み識別情報を抽出し、前記印刷済み識別情報が存在すれば印刷不可と判断し、前記印刷済み識別情報が存在しなければ印刷可と判断する段階と、前記印刷可否判断に従い、前記画像データに基づいて印刷物を出力する段階と、印刷物を出力した画像データの印刷済み識別情報を生成する段階と、前記生成した印刷済み識別情報を、前記印刷物発行端末からネットワークを介して前記サーバへ送信する段階と、前記印刷済み識別情報を前記サーバのデータベースに保存する段階とを含むことを特徴とする印刷物発行方法。

【請求項 17】 印刷物を出力する段階の後に、前記印刷物発行端末に記憶した画像データを削除する段階を更に含むことを特徴とする請求項 16 に記載の印刷物発行

方法。

【請求項 18】 前記画像データの改竄を検出したときに、改竄の検出を出力する段階を更に含むことを特徴とする請求項 16 または 17 のうちのいずれか 1 項に記載の印刷物発行方法。

【請求項 19】 前記画像データを送信する段階の前に、特定の情報を電子透かしとして前記画像データに埋め込む段階を更に含むことを特徴とする請求項 16、17、または 18 のうちのいずれか 1 項に記載の印刷物発行方法。

【請求項 20】 前記画像データを送信する段階の後に、特定の情報を電子透かしとして前記画像データまたは前記印刷物の出力に埋め込む段階を更に含むことを特徴とする請求項 16、17、18、または 19 のうちのいずれか 1 項に記載の印刷物発行方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、印刷物発行端末、サーバ、及び印刷物発行方法に係り、特に、画像データの改竄、漏洩を防止して画像データの原本性を保証するための、ネットワークを介した印刷物発行端末、サーバ、及び印刷物発行方法に関する。

【0002】

【従来の技術】ネットワークを介して手形や小切手等の証券を発行する従来のシステムは、例えば特開 2000-293739 号公報に開示されている。この公報に記載される証券発行装置は、証券を発行する際に、当該証券の発行データを照会することを許可するための照会識別情報を証券毎に生成する生成手段と、この生成手段により生成された証券毎の照会識別情報と、当該各証券の発行データとを対応付けて記憶する記憶手段と、この記憶手段に記憶された発行データと照会識別情報とを印刷手段により証券に印刷させる印刷制御手段と、を備えたことを特徴とする。上記公報では、このような構成により、証券の所持人は、証券の記載内容を見ることによって固有情報を容易に認識することが可能となり、当該証券の真偽を確認するための照会に必要な情報の入力を迅速且つ適確に行うことができる、としている。

【0003】上記従来技術のシステムでは、サーバとネットワークで結ばれたクライアントが証券の発行処理を行う際に、サーバが証券の発行データとクライアントから送信された照会識別情報とが一致するかの判別を行って証券発行データの送信可否を判定している。

【0004】

【発明が解決しようとする課題】しかし、証券会社や銀行などの本店などに備えたサーバから、ネットワークを介して支店などに証券画像データを送信し、支店などで証券を印刷出力するにあたっては、以下の行為が問題となる。すなわち、支店などに備えた証券発行端末に保存されたデータが、権限のない者に閲覧されたり、持ち

出されたり、改竄されたり、複数枚印刷されるなどといった不正行為である。証券画像データの持ち出しは、更に暗号処理方法の解析などに悪用されるおそれもある。上記従来の技術では、このような証券画像の保存データの漏洩、改竄や、印刷された証券の複製、改竄等の不正行為を防止することはできなかった。

【0005】そこで本発明は、サーバからネットワークを介して画像データを送信し、これを受信する印刷物発行端末により手形、証券、小切手等の画像データを出力するにあたり、画像データの漏洩、改竄や、出力された印刷物の複製、改竄等の不正行為を防止できる印刷物発行端末、サーバ、及び印刷物発行方法を提供することを目的とする。

【0006】

【課題を解決するための手段】上記目的を達成するための本発明の印刷物発行端末は、ネットワークを介して画像データをサーバから受信するデータ受信部と、画像データから印刷済み識別情報を抽出し、印刷済み識別情報が存在すれば印刷不可と判断し、印刷済み識別情報が存在しなければ印刷可と判断する印刷可否判断部と、印刷可否判断部の判断に従い、画像データに基づいて印刷物を出力する印刷出力部と、印刷物を出力した後に、画像データの印刷済み識別情報を生成する識別情報生成部と、生成した印刷済み識別情報を、ネットワークを介してサーバへ送信するデータ送信部とを有することを特徴とする。

【0007】このような構成により、出力される印刷物は原本の 1 通のみとなり、印刷物を複数出力する不正行為を防止することができる。

【0008】また、上記目的を達成するための本発明の他の印刷物発行端末は、上記構成で更に、サーバから受信した画像データを記憶するデータ記憶部と、データ記憶部に記憶された画像データを削除するデータ削除部とを有し、印刷出力部は、データ記憶部に記憶された画像データに基づいて印刷物を出力するとともに、データ削除部は、印刷出力部が印刷物を出力した後に、データ記憶部に記憶された画像データを削除することを特徴とする。

【0009】このようにデータ削除部を追加することにより、一端印刷物発行端末内に保存された画像データは、出力後に、または、出力しないと判断された後に不要になれば削除され、画像データの不正な流用や、権限のない者の閲覧、不正な複製、盗難などを防止することができる。画像データの削除が完了したときは、その旨を表示したり、その旨を音声出力したりする機能を付加してもよい。

【0010】ここで画像データの削除とは、ハードディスクなどの記録メディアから画像データファイルを削除することをいう。単なるファイルインデックス情報の削除だけでなく、その物理的な痕跡を残さずに記録メデイ

アから完全に削除することが望ましい。

【0011】上記識別情報生成部が生成する印刷済み識別情報は、画像データから生成された電子署名データを少なくとも含むことが望ましい。この電子署名データは、ハッシュ関数を利用して画像データから生成することができる。また、データ送信部が送信する印刷済み識別情報は、これに加えて画像データの通し番号、及び／または、印刷物発行端末番号を更に含んでいてもよい。

【0012】本明細書において「ハッシュ関数」とは、コリジョン (Collision; 衝突。例えば、 $x \neq y$ のとき $H(x) = H(y)$ となること。) を見つけることが計算量的に困難な関数をいう。比較的短い固定長の電子署名データは、任意長の証券画像データからこのハッシュ関数を利用して生成され、個々の証券画像データに特有と見なされる情報となる。

【0013】また、上記目的を達成するための本発明の他の印刷物発行端末は、上記いずれかの構成で更に、特定の情報を電子透かしとして画像データに埋め込む電子透かし埋め込み部を更に有し、印刷出力部は、電子透かしを埋め込んだ印刷物を出力することを特徴とする。このような構成により、出力された印刷物の改竄、不正な複製の発見、防止ができる。

【0014】ここで「電子透かし」とは、例えば特開平 10-200743 号公報等に記載される方法などにより、印刷物の画像中に特定の情報を埋め込む技術をいう。電子透かしとして埋め込まれる特定の情報には、例えば、日時、場所、オペレータ名などを任意に採用すればよい。本発明における電子透かし埋め込みの方法、方式は、特に限定されない。

【0015】また、上記目的を達成するための本発明の他の印刷物発行端末は、上記いずれかの構成で更に、サーバより受信した公開鍵暗号方式によって暗号化された画像データを復号する復号部を有し、暗号化された画像データを復号部が復号する際に、あらかじめ IC カード、パスワード、または、バイオメトリクスによってオペレータの認証が行われる。

【0016】このような構成により、画像データの漏洩、複製、改竄が防止できる。本明細書において「バイオメトリクス」とは、個々人の生体固有の情報を使って認証を行う方式をいう。例えば、指紋や声紋、虹彩を利用する技術などが知られている。

【0017】本発明において、暗号化の際に使用する公開鍵暗号方式は特に限定されない。また暗号には、例えば、RSA 暗号、楕円曲線暗号、ElGamal 暗号などのアルゴリズムが任意に採用できる。

【0018】また、上記目的を達成するための本発明の他の印刷物発行端末は、上記いずれかの構成で更に、電子透かしを用いて改竄検出を行う改竄検出部を有し、改竄検出部が画像データの改竄を検出したときに、データ送信部は改竄検出情報をサーバに送信することを特徴と

する。

【0019】このような構成により、画像データの改竄などの不正行為を知ることができ、不正行為に対して早期に対応することができる。

【0020】上記目的を達成するための本発明のサーバは、画像データを保存するデータベースと、印刷物発行端末からの照会情報、及び、印刷物発行端末が生成した印刷済み識別情報を、印刷物発行端末よりネットワークを介して受信するデータ受信部と、ネットワークを介して、印刷物発行端末からの照会情報に応じてデータベースに保存される画像データと、印刷物発行端末により生成された印刷済み識別情報が既に存在している場合に、当該印刷済み識別情報とを、印刷物発行端末へ送信するデータ送信部とを有することを特徴とする。

【0021】このような構成により、印刷物発行端末から出力される印刷物は原本の 1 通のみとなり、印刷物を複数出力する不正行為を防止することができる。

【0022】上記データ送信部が送信する印刷済み識別情報は、少なくとも画像データから生成された電子署名データを含むことが望ましく、画像データの通し番号、及び／または、印刷物発行端末番号を更に含んでいてもよい。また、この電子署名データは、前述のハッシュ関数を利用して画像データから生成することができる。

【0023】また、上記目的を達成するための本発明の他のサーバは、上記構成で更に、特定の情報を電子透かしとして画像データに埋め込む電子透かし埋め込み部を有し、電子透かしを埋め込んだ画像データをデータ送信部よりネットワークを介して印刷物発行端末へ送信する機能を有することを特徴とする。

【0024】このような構成により、印刷可否判断情報や画像データの改竄、不正な複製の発見、防止ができる。ここで画像データに電子透かしで埋め込まれる特定の情報は、例えば、日時、場所、オペレータ名などを任意に採用すればよい。

【0025】また、上記目的を達成するための本発明の他のサーバは、上記いずれかの構成で更に、画像データを公開鍵暗号方式によって暗号化する暗号化部を有することを特徴とする。また、暗号化に用いる公開鍵は、あらかじめ認証局がオペレータの本人確認を行った上で発行する公開鍵証明書によって、オペレータ本人の公開鍵であることが証明されている公開鍵を用いることを特徴とする。

【0026】このような構成により、画像データの漏洩、複製、改竄が防止できる。本発明において、暗号化の際に使用する公開鍵暗号方式は特に限定されず、また暗号には、例えば、RSA 暗号、楕円曲線暗号、ElGamal 暗号などのアルゴリズムを任意に採用できる。

【0027】上記目的を達成するための本発明の印刷物発行方法は、ネットワークを介して画像データをサーバから印刷物発行端末へ送信する段階と、画像データから

印刷済み識別情報を抽出し、印刷済み識別情報が存在すれば印刷済み識別情報の正当性を確認し、正当であると確認できれば印刷不可と判断し、正当であると確認できなければ不正ありと判断してオペレータに通知し、印刷済み識別情報が存在しなければ印刷可と判断する段階と、印刷可否判断に従い、画像データに基づいて印刷物を出力する段階と、印刷物を出力した画像データの印刷済み識別情報を生成する段階と、生成した印刷済み識別情報を、印刷物発行端末からネットワークを介してサーバへ送信する段階と、印刷済み識別情報をサーバのデータベースに保存する段階とを含むことを特徴とする。

【0028】このような構成により、出力される印刷物は原本の1通のみとなり、印刷物を複数出力する不正行為を防止することができる。

【0029】また、上記目的を達成するための本発明の他の印刷物発行方法は、上記構成で印刷物を出力する段階の後に、印刷物発行端末に記憶した画像データを削除する段階を更に含むことを特徴とする。

【0030】このように画像データを削除する段階を追加することにより、一端印刷物発行端末内に保存された画像データは、印刷出力後に、または、印刷しないと判断された後に不要になれば削除され、画像データの不正な流用や権限のない者の閲覧、盗難、不正な複製などを防止することができる。

【0031】また、上記目的を達成するための本発明の他の印刷物発行方法は、上記いずれかの構成で更に、画像データの改竄を検出したときに、改竄の検出を出力する段階を含むことを特徴とする。

【0032】ここで出力とは、画像表示、音声出力、印刷出力、サーバへの送信などであり、特に限定されない。このような構成により、不正行為を知ることができる。不正行為に対して早期に対応することができる。

【0033】また、上記目的を達成するための本発明の他の印刷物発行方法は、上記いずれかの構成で更に、画像データを送信する段階の前に、または、画像データを送信しこれを印刷物発行端末が受信した後に、特定の情報を電子透かしとして画像データに埋め込む段階を含むことを特徴とする。このような構成により、画像データや出力された印刷物の改竄、不正な複製の発見、防止ができる。

【0034】ここで電子透かしは画像データ中に埋め込んでもよく、また、印刷物のイメージ中に埋め込んでもよい。印刷物のイメージ中に埋め込む方法は、例えば前述の特開平10-200743号公報等に記載される方法などが利用できる。電子透かしとして埋め込まれる特定の情報は、例えば、日時、場所、オペレータ名などを任意に採用すればよい。本発明における電子透かし埋め込み方法、方式は、特に限定されない。

【0035】本発明においてネットワークとは、インターネット、専用回線、LAN、WAN、電話通信網、無

線通信網、双方向放送網等を含み、特に限定されない。また、本発明の印刷物発行端末は、唯一のサーバに対応してシステムが構成されていてもよく、また、複数のサーバに対応してシステムが構成されていてもよい。更に、本発明の印刷物発行端末は、単独の端末が存在してシステムが構成されていてもよく、また、複数端末が同時に存在してシステムが構成されていてもよい。

【0036】

【発明の実施の形態】以下に、本発明のいくつかの実施の形態を、図面を用いて説明する。なお、本明細書及び図面において、実質的に同一の機能構成を有する構成要素については同一の符号を付することにより重複説明を省略する。

【0037】（第1の実施形態）図1は、本発明の第1の実施形態にかかる証券発行方法を説明する概念図である。証券発行端末100は、データ受信部101、データ記憶部102、印刷可否判断部103、印刷出力部104、識別情報生成部105、及びデータ送信部106を少なくとも含んで構成される。一方、証券照会サーバ120は、証券データベース121、データ受信部122、及びデータ送信部123を少なくとも含んで構成される。証券発行端末100及び証券照会サーバ120は、ネットワーク110を介して相互にアクセス可能である。

【0038】図2は、第1の実施形態の証券発行の手続の流れを示すフローチャートである。まず、ステップS101で、端末が設置された支店等にてオペレータが証券発行端末100から証券照会サーバ120へ、証券画像データのリストをネットワーク110を介して照会する（S101）。この照会をデータ受信部122で受けた証券照会サーバ120は、証券画像データベース121に存在する証券画像データのリストを証券発行端末100に返す。そして、ステップS102で、オペレータはこのリストの中から印刷出力したい証券を証券通し番号で指定して選択し、更に証券照会サーバ120へ送信する（S102）。

【0039】次に、ステップS103で、証券照会サーバ120は選択された証券画像データ（図示せず）を、データ送信部123からネットワーク110を介して証券発行端末100へ送信する（S103）。証券発行端末100のデータ受信部101はこれを受信し、データ記憶部102はこれを記憶する。

【0040】次に、ステップS104で、証券発行端末100の印刷可否判断部103は、印刷済み識別情報600の存在の有無を確認する（S104）。

【0041】図11は、印刷済み識別情報600の構成の一例である。ここでは、印刷済み識別情報600は、証券画像データ識別番号部600a、電子署名データ部600b、及び証券発行端末番号部600cの組で構成される。印刷済み識別情報600の電子署名データ部6

00bは、対応する証券画像データからハッシュ関数を利用して生成する。

【0042】次に、ステップS105で、もし印刷済み識別情報600が存在しなければ、ステップS106で、証券発行端末100の印刷出力部104より、証券を印刷出力する(S105, S106)。

【0043】次に、ステップS107で、証券発行端末100の識別情報生成部105が、印刷済み識別情報600を生成する(S107)。そして、ステップS108で、証券発行端末100のデータ送信部106が、印刷済み識別情報600を証券照会サーバ120に送信する(S108)。証券照会サーバ120のデータ受信部122は、印刷済み識別情報600を受信し、これが証券データベース121に保存される。そして手続は終了する。

【0044】ステップS105で、もし印刷済み識別情報600が存在すれば、次にステップS109で電子署名データ部600bの確認を行う。そして、電子署名が確認できれば手続は終了する。もしステップS109で電子署名が確認できなければ、次にステップS110でオペレータに不正ありの通知を行い手続は終了する。

【0045】このような証券発行方法により、印刷される証券は原本の1通のみとなり、証券を複数印刷する不正行為を防止することができる。

【0046】(第2の実施形態)図3は、本発明の第2の実施形態にかかる証券発行方法を説明する概念図である。証券発行端末200は、データ受信部201、データ記憶部202、印刷可否判断部203、印刷出力部204、識別情報生成部205、データ送信部206、及びデータ削除部207を少なくとも含んで構成される。一方、証券照会サーバ220は、証券データベース221、データ受信部222、及びデータ送信部223を少なくとも含んで構成される。証券発行端末200及び証券照会サーバ220は、ネットワーク210を介して相互にアクセス可能である。

【0047】図4は、第2の実施形態の証券発行の手続の流れを示すフローチャートである。ステップS201からステップS210までの流れは、第1の実施形態(図2)の、ステップS101からステップS110までの流れと同様であるので説明を省略する。

【0048】ステップS208の終了後、または、ステップS205で肯定分岐のときは、ステップS211で、証券発行端末200のデータ削除部207が、データ記憶部202の証券画像データを削除する(S211)。そして手続は終了する。

【0049】このようにデータ削除の工程を追加した証券発行方法により、第1の実施形態の効果と同様、印刷される証券は原本の1通のみとなり、証券を複数印刷する不正行為を防止することができる。そして更に、一端証券発行端末内に保存された証券画像データは、印刷出

力後に、または、印刷しないと判断された後に不要になれば削除され、証券画像データの不正な流用や権限のない者の閲覧、不正な複製、盗難などを防止することができる。

【0050】(第3の実施形態)図5は、本発明の第3の実施形態にかかる証券発行方法を説明する概念図である。証券発行端末300は、データ受信部301、データ記憶部302、印刷可否判断部303、印刷出力部304、識別情報生成部305、データ送信部306、データ削除部307、及び改竄検出部308を少なくとも含んで構成される。一方、証券照会サーバ320は、証券データベース321、データ受信部322、データ送信部323、及び電子透かし埋め込み部324を少なくとも含んで構成される。証券発行端末300及び証券照会サーバ320は、ネットワーク310を介して相互にアクセス可能である。

【0051】図6は、第3の実施形態の証券発行の手続の流れを示すフローチャートである。まず、ステップS301で、端末が設置された支店等にてオペレータが証券発行端末300から証券照会サーバ320へ、証券画像データのリストをネットワーク310を介して照会する(S301)。この照会をデータ受信部322で受けた証券照会サーバ320は、証券画像データベース321に存在する証券画像データのリストを証券発行端末300に返す。そして、ステップS302で、オペレータはこのリストの中から印刷出力したい証券を証券通し番号で指定して選択し、更に証券照会サーバ320へ送信する(S302)。

【0052】次に、ステップS303で、証券照会サーバ320の電子透かし埋め込み部324が、証券画像データに特定のデータを電子透かしによって埋め込む(S303)。

【0053】次に、ステップS304で、証券照会サーバ320は、選択され、電子透かしが埋め込まれた証券画像データを、データ送信部323からネットワーク310を介して証券発行端末300へ送信する(S304)。

【0054】ステップS305から終了までの流れは、第2の実施形態(図4)の、ステップS204から終了までの流れと同様であるので説明を省略する。

【0055】電子透かし技術を利用すれば、例えば、ある一定以上の解像度の情報を透かし技術によって埋め込んだ印刷物は、複製を行った場合に、一定の解像度以上の情報を正しく読み取ることができない。従って、複製印刷の際に埋め込まれた情報が正しく印刷できず、電子透かしの検出を行った際に埋め込まれた情報を検出できなくなる。これを利用して不正な複製を検出することができる。

【0056】本実施形態では、複製が行われる際に読み取ることが困難な電子透かし情報を証券画像に埋め込

み、電子透かし情報が正しく印刷されているかどうかを調べることで、不正な複製が行われていないかどうかの判断が可能になる。

【0057】また、改竄が行なわれた場合は、埋め込まれた情報が改竄によって隠されてしまう。このため、電子透かしの検出を行った際に埋め込まれた情報が検出できなくなる。従って改竄が行われていることが検出できる。

【0058】このように、第3の実施形態の証券発行方法により、第1の実施形態及び第2の実施形態の効果に加え、印刷出力された証券の改竄、不正な複製の発見、防止ができる効果がある。

【0059】（第4の実施形態）図7は、本発明の第4の実施形態にかかる証券発行方法を説明する概念図である。証券発行端末400は、データ受信部401、データ記憶部402、印刷可否判断部403、印刷出力部404、識別情報生成部405、データ送信部406、データ削除部407、及び改竄検出部408、復号部409を少なくとも含んで構成される。一方、証券照会サーバ420は、証券データベース421、データ受信部422、データ送信部423、及び暗号化部425を少なくとも含んで構成される。証券発行端末400及び証券照会サーバ420は、ネットワーク410を介して相互にアクセス可能である。また、証券発行端末400及び証券照会サーバ420から、ネットワーク410を介して認証局700にアクセス可能である。

【0060】図8は、第4の実施形態の証券発行の手続の流れを示すフローチャートである。ステップS401、ステップS402の流れは、第1の実施形態（図2）のステップS101、ステップS102の流れと同様であるので説明を省略する。

【0061】次に、ステップS403で、証券照会サーバ420の暗号化部425が、証券画像データを公開鍵暗号方式によって暗号化する（S403）。暗号化に用いる公開鍵は、オペレータ自身が証券照会サーバ420に提供するか、または認証局700より公開鍵証明書を取得することで入手できる。

【0062】次に、ステップS404で、証券照会サーバ420は、選択され、暗号化された証券画像データを、データ送信部423からネットワーク410を介して証券発行端末400へ送信する（S404）。

【0063】次に、ステップS405で、証券発行端末400の復号部409が、暗号化されている証券画像データを復号する（S405）。

【0064】暗号化された証券画像データを復号部409が復号する際には、オペレータの認証が行われる。オペレータの認証は、前述したように、ICカード、パスワード、または、バイオメトリクスにより行う。復号に用いる秘密鍵は証券発行端末400に保存されるか、または、証券発行端末400のオペレータがICカード内

に保持していればよい。対応する公開鍵の提供を認証局700が行う場合、認証局700は書面やオンライン利用によるオペレータ本人の確認を行い、公開鍵証明書を発行する。発行された公開鍵証明書には公開鍵が含まれ、証券照会サーバ420がネットワーク410を介して入手することができる。

【0065】ステップS406から終了までの流れは、第2の実施形態（図4）の、ステップS204から終了までの流れと同様であるので説明を省略する。

【0066】このような第4の実施形態の構成により、第2の実施形態の効果に加え、証券画像データの漏洩、複製、改竄が防止できる効果がある。

【0067】（第5の実施形態）図9は、本発明の第5の実施形態にかかる証券発行方法を説明する概念図である。証券発行端末500は、データ受信部501、データ記憶部502、印刷可否判断部503、印刷出力部504、識別情報生成部505、データ送信部506、データ削除部507、及び電子透かし埋め込み部509を少なくとも含んで構成される。一方、証券照会サーバ520は、証券データベース521、データ受信部522、及びデータ送信部523を少なくとも含んで構成される。証券発行端末500及び証券照会サーバ520は、ネットワーク510を介して相互にアクセス可能である。

【0068】図10は、第5の実施形態の証券発行の手続の流れを示すフローチャートである。ステップS501からステップS505までの流れは、第1の実施形態（図2）のステップS101からステップS105までの流れと同様であるので説明を省略する。

【0069】次に、ステップS506で、証券発行端末500の電子透かし埋め込み部509が、証券画像データに特定のデータを電子透かしによって埋め込む（S506）。

【0070】ステップS507から終了までの流れは、第2の実施形態（図4）の、ステップS206から終了までの流れと同様であるので説明を省略する。

【0071】第3の実施形態では、証券画像データへの電子透かしの埋め込みを、証券照会サーバにて行ったが、第5の実施形態では、証券発行端末にて行う。電子透かし埋め込みの効果については第3の実施形態と同様である。従って、第5の実施形態の証券発行方法によれば、第1の実施形態及び第2の実施形態の効果に加え、印刷出力された証券の改竄、不正な複製の発見、防止ができる効果がある。

【0072】以上、添付図面を参照しながら本発明の証券発行端末、証券照会サーバ、及び証券発行方法の好適な実施形態について説明したが、本発明はこれらの例に限定されない。いわゆる当業者であれば、特許請求の範囲に記載された技術的思想の範疇内において各種の変更例または修正例に想到し得ることは明らかであり、それ

らについても当然に本発明の技術的範囲に属するものと了解される。

【0073】また、本発明は、手形や小切手などの証券に限って説明したが、本発明がこれら以外の原本保証性が要求される書類にも適用できることはいうまでもない。本発明は、証券の印刷に限らず、証券以外の公文書や領収書、一般文書等のあらゆる文書、ロゴマーク、写真等のすべての画像についての印刷にも適用することができる。

【0074】

【発明の効果】以上説明したように、本発明によれば、証券照会サーバからネットワークを介して証券発行端末により手形や小切手等の証券を印刷出力するにあたり、証券画像の保存データの漏洩、改竄や、印刷された証券の複製、改竄等の不正行為を防止できる証券発行端末、証券照会サーバ、及び証券発行方法が提供できた。

【図面の簡単な説明】

【図1】図1は、第1の実施形態にかかる証券発行方法を説明する概念図である。

【図2】図2は、第1の実施形態の証券発行の手続の流れを示すフローチャートである。

【図3】図3は、第2の実施形態にかかる証券発行方法を説明する概念図である。

【図4】図4は、第2の実施形態の証券発行の手続の流れを示すフローチャートである。

【図5】図5は、第3の実施形態にかかる証券発行方法を説明する概念図である。

【図6】図6は、第3の実施形態の証券発行の手続の流れを示すフローチャートである。

【図7】図7は、第4の実施形態にかかる証券発行方法を説明する概念図である。

【図8】図8は、第4の実施形態の証券発行の手続の流れを示すフローチャートである。

【図9】図9は、第5の実施形態にかかる証券発行方法を説明する概念図である。

【図10】図10は、第5の実施形態の証券発行の手続

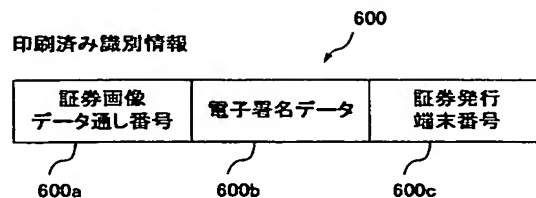
の流れを示すフローチャートである。

【図11】図11は、印刷済み識別情報600の構成の一例である。

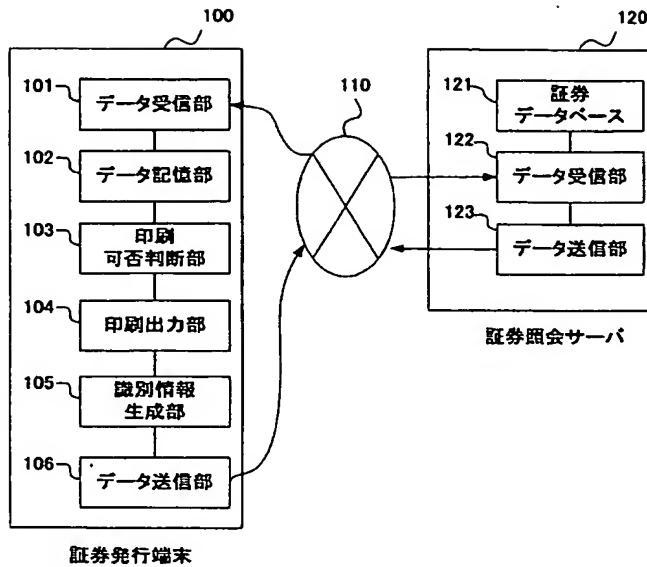
【符号の説明】

100, 200, 300, 400, 500	証券発行
端末	
101, 201, 301, 401, 501	データ受
信部	
102, 202, 302, 402, 502	データ記
憶部	
103, 203, 303, 403, 503	印刷可否
判断部	
104, 204, 304, 405, 505	印刷出力
部	
105, 205, 305, 405, 505	識別情報
生成部	
106, 206, 306, 406, 506	データ送
信部	
207, 307, 407, 507	データ削除部
308, 408	改竄検出部
409	復号部
324, 509	電子透かし埋め込み部
110, 210, 310, 410, 510	ネットワ
ーク	
120, 220, 320, 420, 520	証券照会
サーバ	
121, 221, 321, 421, 521	証券デー
タベース	
122, 222, 322, 422, 522	データ受
信部	
123, 223, 323, 423, 523	データ送
信部	
425	暗号化部
600	印刷済み識別情報
700	認証局

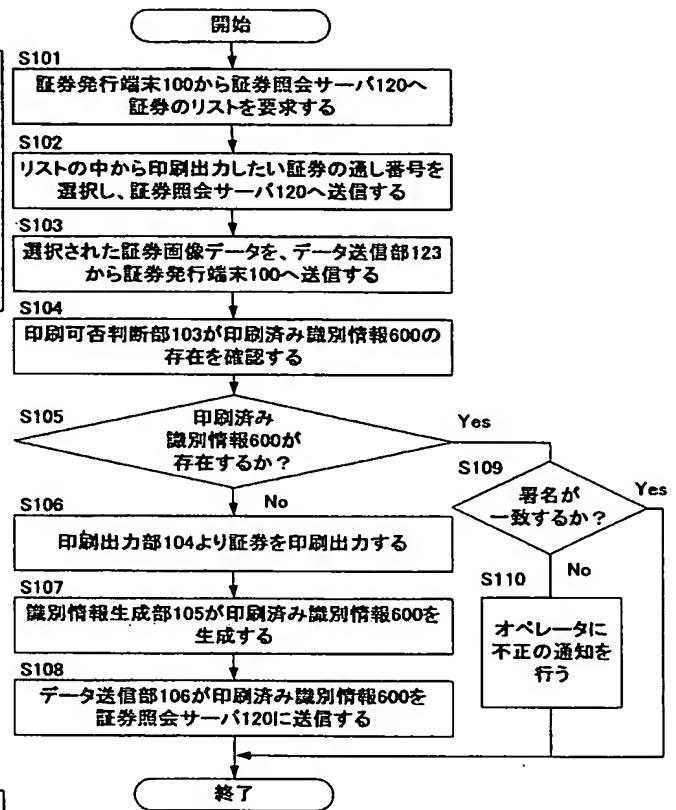
【図11】



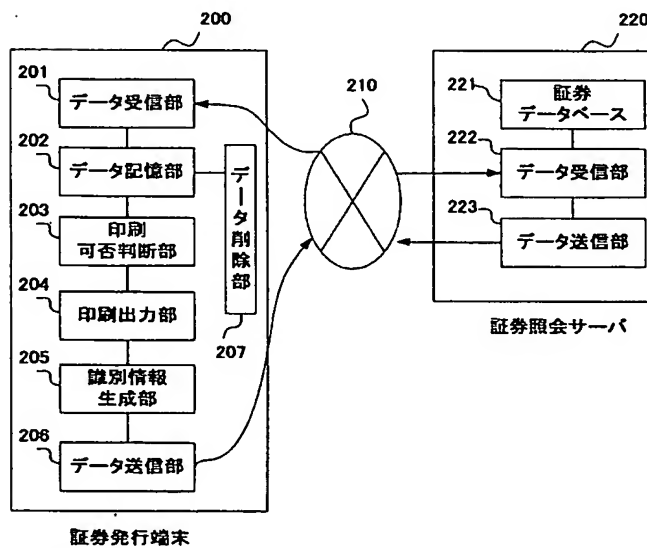
【図1】



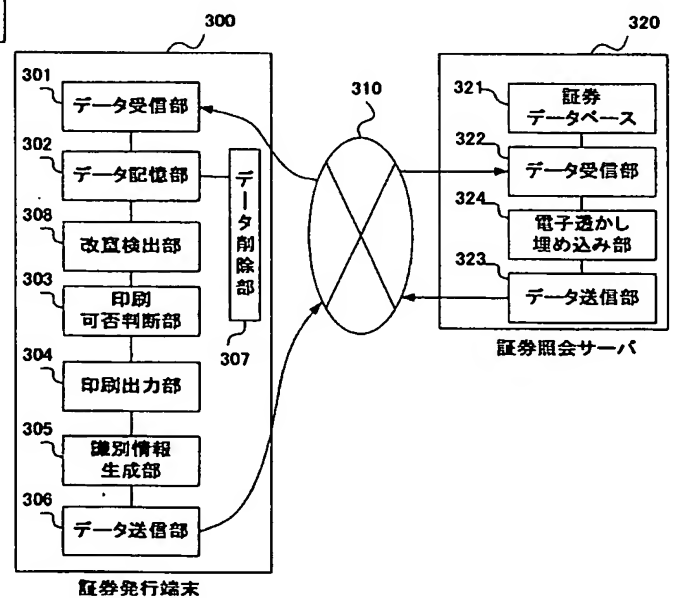
【図2】



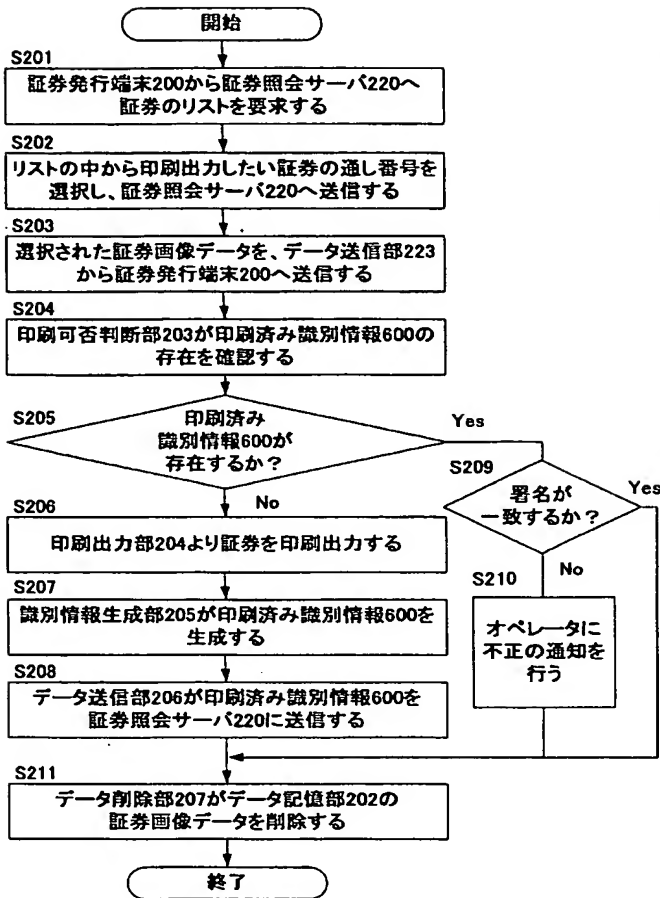
【図3】



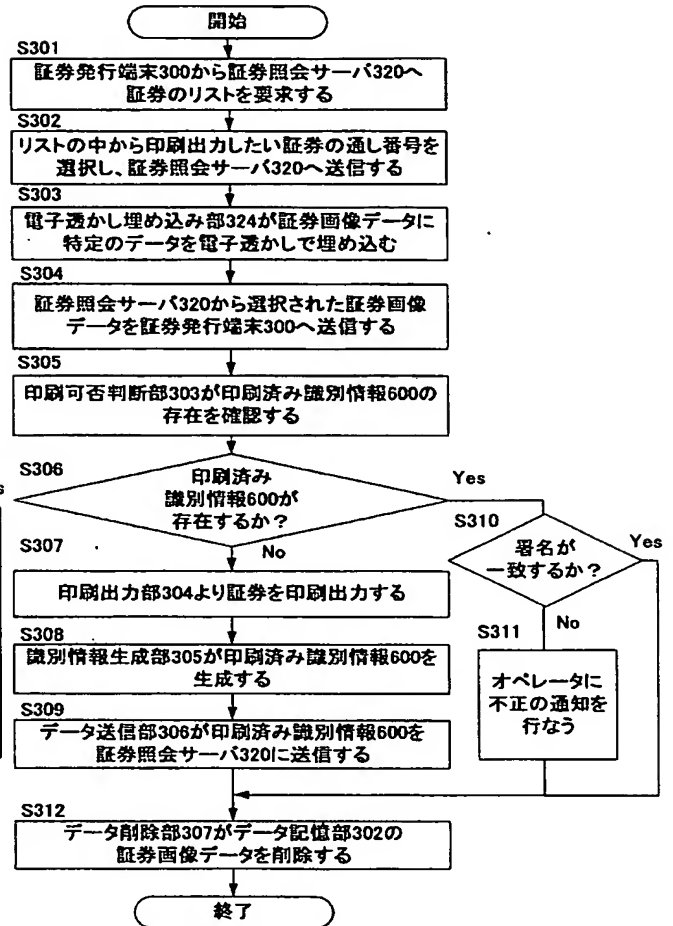
【図5】



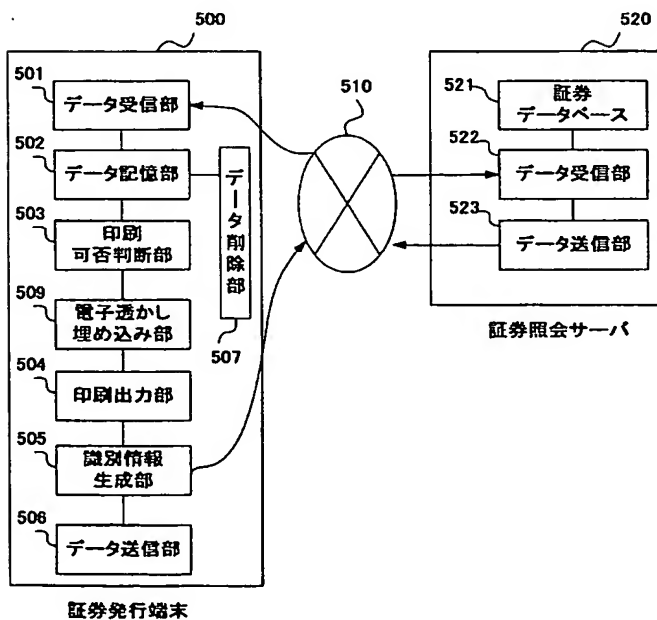
【図4】



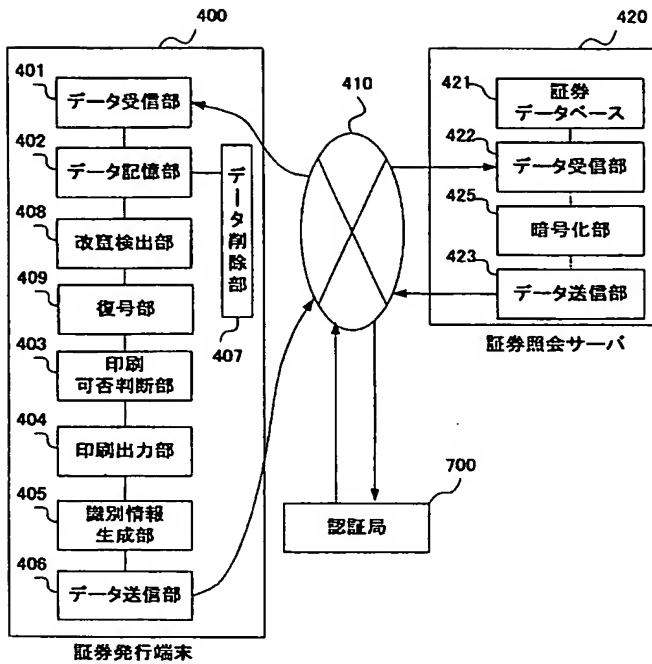
【図6】



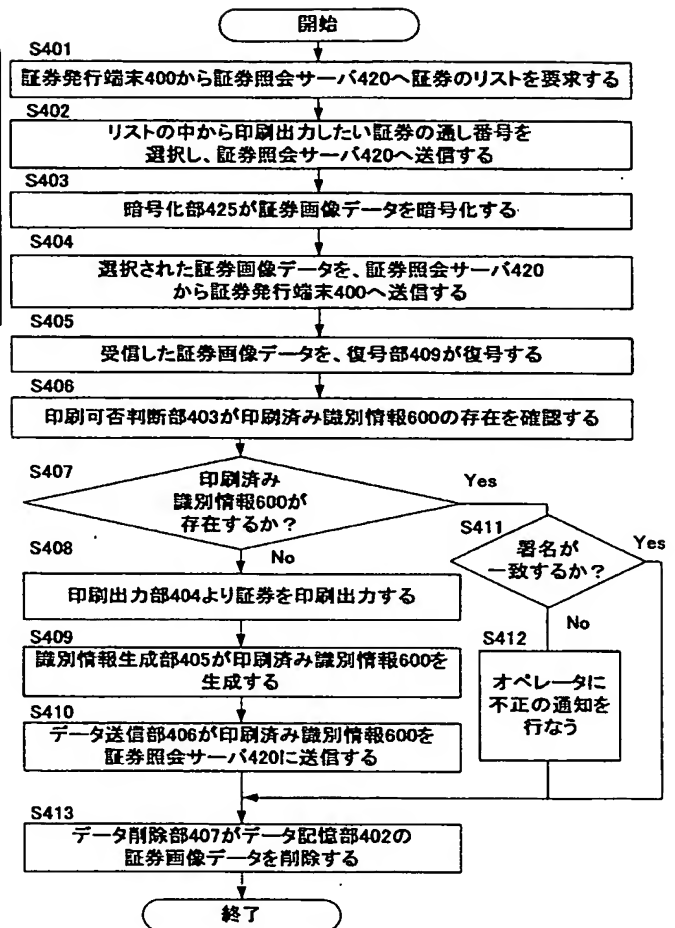
【図9】



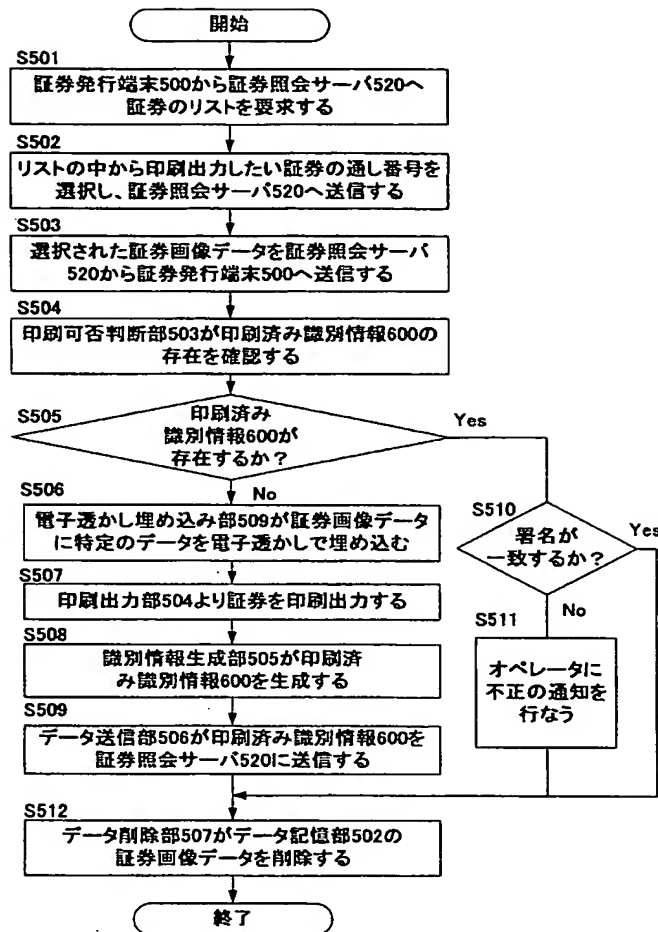
【図7】



【図8】



【図10】



フロントページの続き

(51) Int. Cl. ⁷	識別記号	F I	テーマコード(参考)
H 0 4 N 1/00		H 0 4 N 1/00	1 0 7 Z 5 C 0 7 6
	1 0 7	1/387	
1/387		B 4 1 J 29/00	Z

(72)発明者 塚本 明利
 東京都港区虎ノ門1丁目7番12号 沖電気
 工業株式会社内

Fターム(参考) 2C061 AP01 CL08 HH01 HH03 HJ06
 HK11 HN05 HN23
 2C187 AE07 AE20 BF19 BF26 BF34
 GC09 GD02 GD06
 5B021 AA11 NN18 NN19
 5B057 AA11 CB19 CE08
 5C062 AA02 AA05 AA29 AB38 AC21
 AC41 AC42 AC43 AC58 AF00
 BA00
 5C076 AA14 BA06